UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,904	12/01/2000	Bjorn Markus Jakobsson	38-2	3689

7590	07/27/2004

Joseph B. Ryan
Ryan, Mason & Lewis, LLp
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER
BAYAT, BRADLEY B

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 07/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. Box 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Paper No. 11

Application Number: 09/727,904
Filing Date: December 01, 2000
Appellant(s): JAKOBSSON ET AL.

MAILED

JUL 2 ...

GROUP 3600

Joseph B. Ryan for
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on April 28, 2004.

(1)   *Real Party in Interest*

A statement identifying the real party in interest is contained in the brief.

(2)   *Related Appeals and Interferences*

The brief contains a statement that there are no related appeals or interferences.

(3)   *Status of Claims*

The statement of the status of the claims contained in the brief is correct.

(4)   *Status of Amendments After Final*

The appellant's statement of the status of amendments after final rejection contained in

the brief is correct.

(5)   *Summary of Invention*

The summary of invention contained in the brief is correct.

(6)   *Issues*

The appellant's statement of the issues in the brief is substantially correct. The changes

are as follows:

1. Whether claims 1-4 and 7-20 are unpatentable under 35 U.S.C. §103(a) over U.S.

Patent No. 5,754,656 (hereinafter "Nishioka") in view of U.S. Patent No. 6,275,936 (hereinafter

"Kyojima").

2. Whether claims 5 and 6 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent

No. 5,754,656 (hereinafter "Nishioka") in view of U.S. Patent No. 6,275,936 (hereinafter

"Kyojima") in further view of U.S. Patent No. 6,396,928 (hereinafter "Zheng").

(7)   Grouping of Claims

Appellant's brief includes a statement that claims 1, 4-6, 8, 9 and 15-17 stand or fall

together; claims 2, 3, 7 and 10-14 each stand or fall alone, and claims 18-20 stand or fall

together.

(8)   Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9)   Prior Art of Record

5,754,656	Nishioka et al.	5-1998
6,275,936 B1	Kyojima et al.	8-2001
6,396,928 B1	Zheng	5-2002

(10)   Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-4, 7-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Nishioka et al. (hereinafter Nishioka, U.S. Patent 5,754,656) in view of Kyojima et al.

(hereinafter Kyojima, U.S. Patent 6,275,936 B1).

As per **Claim 1**, Nishioka discloses a method for controlling access to one or more

information items purchasable from a merchant and accessible over a network, wherein a user

interested in a given information item is permitted to access a corresponding signed ciphertext of

the given information item, the signed ciphertext having at least a first ciphertext portion, the

method comprising the steps of:

-      receiving from the user a first ciphertext portion of the signed ciphertext (column

  13, lines 48-52) in conjunction with a request from the user for purchase of the

  given information item from the merchant (column 3, lines 16-61; column 11,

  lines 15-67)

-      decrypting the first ciphertext portion and returning to the user the resulting

  decrypted version of the first ciphertext portion, wherein the resulting decrypted

  portion provides information that is utilized by the user in conjunction with

  accessing the given information item in a manner such that the merchant is unable

  to identify the given information item purchased by the user (column 2, lines 33-

  67; column 7, lines 42-62).

Nishioka does not explicitly disclose the use of a blinded ciphertext technique. Kyojima

discloses a method and device to authenticate and control access to digital data by applying a

blinding effect and decryption technique to a ciphertext that can securely transmit a specific

piece of information to a decryption device while keeping the blindness of the data to be

delegated (see column 4, lines 57-65; columns 6 lines 1-7, 33-45; column 8, lines 5-41).

Kyojima is evidence that one of ordinary skill in the art would recognize the benefit of utilizing a

blind ciphertext decryption technique to provide for access to digital data yet at the same time

disclose only the information necessary to perform the intended transaction, while at the same

time protecting the "challenging data", i.e., user identity, specific fees or purchase price (column

11, lines 25-65; column 12, line 10-18). It would have been obvious to one of ordinary skill in

the art at the time of applicant's invention to modify the method of Nishioka and include the

blind decryption technique because it would provide further privacy to a user purchasing an

information item since the content of the delegated encrypted key and the decryption key of the

digital data cannot be known to the proving device, as per teachings of Kyojima. In fact,

Kyojima provides motivation by indicating the "privacy of a recipient of data as to what kind of

data he/she would like to decrypt is recorded by the decryption device and later used

illegitimately (column 2, lines 2-4)." Furthermore, Kyojima points out that the seriousness of the

problem is amplified when decryption of data is occurring over a network and anyone can learn

the result of the decryption (e.g., purchased information item) without the blinding effect

(column 2, lines 15-25).

As per **claim 2**, Nishioka further discloses the method of claim 1 wherein the signed

ciphertext for the given information item comprises the first ciphertext portion, a second

ciphertext portion, an unencrypted description of the information item, and a tag, with at least a

portion of the tag comprising a signature (column 7, lines 42-62; columns 13-14).

As per **claim 3**, Nishioka further discloses the method of claim 2 wherein the signature

utilizes at least a part of the first ciphertext portion as a public key (column 4, lines 3-17, column

5, lines 15-31).

As per **claim 4**, Nishioka further discloses the method of claim 1 wherein the first

ciphertext portion comprises a symmetric key encrypted using a public key associated with the

merchant (figure 5 and associated text).

As per **claim 7**, Nishioka further discloses the method of claim 1 wherein the signed ciphertext further includes a second ciphertext portion corresponding to an encrypted version of the given information item (figures 21, 22 and associated text).

As per **claim 8**, Nishioka further discloses the method of claim 1 wherein the user verifies a signature of the signed ciphertext before requesting purchase of the given information item (figure 12 and associated text).

As per **claim 9**, Nishioka does not disclose that the decrypting step is implemented in a payment server associated with the merchant. Kyojima discloses a decryption method and device and access right authentication method and apparatus wherein the decrypting step is implemented in the payment server (figure 10 and associated text; columns 13-14). It would have been obvious to one of ordinary skill in the art at the time of applicant's claimed invention to modify Nishioka by implementing decryption within the payment server so that further privacy is intact and the blindness of the data or its decryption result can be concealed from any intercepting party or even the proving device itself (column 14, lines 39-44), as per teaching of Kyojima.

As per **claims 10 and 11**, Nishioka does not disclose that the decryption of the blinded version of the first ciphertext portion returned to the user comprises a blinded key or proof of correct decryption that when un-blinded by the user is used to decrypt a second ciphertext portion of the signed ciphertext so as to obtain the purchased information item or to check for correctness. Kyojima discloses a decryption method and device wherein the decryption of the

blinded version of the first ciphertext portion returned to the user comprises a blinded key or

proof of correct decryption that when un-blinded by the user is used to decrypt a second

ciphertext portion of the signed ciphertext so as to obtain the purchased information item or to

check for correctness (column 5; columns 17-19). It would have been obvious to one of ordinary

skill in the art at the time of applicant claimed invention to modify Nishioka to include a blinded

key or proof of correct decryption to provide an additional layer of security for obtaining data

and further protecting the privacy of the user from interception by any third party to determine

the information item purchased by the user.

As per **claims 12-14**, Nishioka does not disclose that the decrypting step is implemented

in at least part of a set of multiple rounds, with the user providing a blinded ciphertext and

receiving a corresponding decryption result for each of the rounds. Kyojima discloses a

decryption method and device wherein the decrypting step is implemented in at least part of a set

of multiple rounds, with the user providing a blinded ciphertext and receiving a corresponding

decryption result for each of the rounds (column 10, line 33- column 11, line 25; column 22,

lines 22-column 23, line 60). It would have been obvious to one of ordinary skill in the art at the

time of applicant claimed invention to modify Nishioka to include multiple round blinding and

decryption technique to provide an additional layer of security for obtaining data and further

protecting the privacy of the user from interception by any third party to determine the

information item purchased by the user.

As per **claim 15**, Nishioka further discloses the method of claim 1 wherein the merchant

establishes different public keys for use with different ones of a plurality of information items

purchasable from the merchant (column 16, line 44 – column 17, line 56).

Claims 16-20 are directed to a machine-readable medium/processor based system/a

method of controlling access exhibiting similar or inclusive of the elements or steps of above

cited claims and are therefore rejected as above.

Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Nishioka et al. (hereinafter Nishioka, U.S. Patent 5,754,656) in view of Kyojima et al.

(hereinafter Kyojima, U.S. Patent 6,275,936 B1) as applied to claim 1 above and in further

view of Zheng, U.S. Patent 6,396,928 B1.

As per **claims 5 and 6,** Nishioka and Kyojima do not explicitly disclose the use of an

ElGamal encryption technique or the Schnorr signature scheme. Zheng teaches a method and

system for performing digital data encryption and signature coding for use in communications

and digital information systems utilizing ElGamal and Schnorr signature encryption schemes

(column 2, lines 14-23; column 4, line 40 – column 5, line 67). Zheng is evidence that one of

ordinary skill in the art would recognize that various encryption techniques can be utilized to

perform data encryption and eventual authentication. It would have been obvious to one of

ordinary skill in the art at the time the invention to modify the inventions of Nishioka and

Kyojima to utilize a method known as "signcryption" wherein an encryption technique and

signature scheme are combined to achieve improved computational efficiency and reduce

message transmission overhead (column 1, lines 24-40), thus lowering the cost of information

dissemination to the merchant while maintaining information privacy and authentication

integrity.

(11)   Response to Argument

As per claims 1 and 2, the Appellant asserts that the examiner has failed to establish a

proper prima facie case of obviousness and that the cited references (Nishioka and Kyojima) fail

to teach or suggest all the claim limitations and that there is no cogent motivation for modifying

the reference teachings to reach the claimed invention (Appellant's brief pages 2-4). Appellant

further contends that after reviewing the entirety of the Kyojima, Appellant was unable to find

"any mention of a signed ciphertext, much less a blinded version of a first ciphertext portion of a

signed ciphertext (Id. at 5)." The Appellant relies on the arguments set forth for claim one

above, because the remaining claims are either dependent on claim one or include at least one

such element.

In response to Appellant's argument that the examiner has "failed to identify a cogent

motivation" and relies on subjective conclusory statements, it must be recognized that any

judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight

reasoning. But so long as it takes into account only knowledge which was within the level of

ordinary skill at the time the claimed invention was made, and does not include knowledge

gleaned only from the Appellant's disclosure, such a reconstruction is proper. See *In re*

McLaughlin, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to Appellant's further argument with respect to claims 1 and 2, that there is no

suggestion to combine the references, the examiner recognizes that obviousness can only be

established by combining or modifying the teachings of the prior art to produce the claimed

invention where there is some teaching, suggestion, or motivation to do so found either in the

references themselves or in the knowledge generally available to one of ordinary skill in the art.

See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347,

21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the cited references are directed to controlling

access and authentication of data utilizing encryption and signature schemes to protect the

privacy of a user from allowing access to information items that are not needed by each party

during the electronic transaction. Therefore, the protection of privacy of the consumer is

tantamount in each reference from either interception by an outsider or illegitimate use by a

merchant and/or a credit card company.

The examiner asserts that Nishioka discloses how entities on a communication network

can utilize cipher communication methods in an electronic shopping system wherein a user

desires to purchase products, however, the user does not desire the contents of the products

purchased to become known to at least one of those entities (see summary columns 1-2).

Nishioka explicitly discloses the need and desire on the part of the user to conduct electronic

commerce without having to disclose the content of the purchase (column 2, lines 24-31).

Nishioka further teaches how combining a digital signature sgnA(P) with predetermined

ciphertext portions (signed cipher) can thereby authenticate the written order P=(P1, P2)

(columns 6-7; figures 11, 12 and associated text). Nishioka teaches how the proper entity is

"notified of only the predetermined information, [accordingly, the] privacy of the user is

protected (column 7, lines 42-62)."

Furthermore, Kyojima recognizes security flaws in the prior art and thus applies a blind

decryption method to securely transmit a specific piece of information to a decryption device

while keeping the blindness of data delegated to be decrypted or to control access to such data (see background of the invention columns 1-4). Kyojima teaches how a decryption device decrypts a cipher text encrypted with of a digital signature (RSA Method), thus forming a signed ciphertext (see column 5-6). Kyojima further discloses that a user of the blind decryption device possesses the cipher text C, a modulus n, the encryption key E (e.g., a digital signature) and the second decryption information d2 (see column 8). Appellant describes the user in the specification as a customer or a processing device (see Appellant's specification page 4). Kyojima further teaches that challenging plain data or its decryption result can be concealed from the proving device itself (columns 13-14).

As per claims 1 and 18-20, the Appellant submits that access to the purchased information item is given to a user in a manner such that the merchant is unable to identify the given information item purchased by the user (Appellant's brief pages 6-7).

Appellant discloses in the specification that although the payment server in the system is associated with the merchant, this is not a requirement of the invention and the payment server may be a third party entity separate from the merchant (specification page 4). Thus Appellant's argument that the merchant is unable to identify the given information item purchased (brief page 6) is in line Kyojima wherein the purchased information item can be concealed from the proving device (column 14). Furthermore, by the blinding technique of Kyojima no one can intercept or decrypt the information item being purchased by the user until the user removes the blind effect to obtain a decryption result (column 8, lines 1-55).

Moreover, Appellant's claim that "information is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user" is a recitation of the intended use of the claimed

invention which must result in a structural difference between the claimed invention and the

prior art in order to patentably distinguish the claimed invention from the prior art. If the prior

art structure is capable of performing the intended use, then it meets the claim. In a claim drawn

to a process of making, the intended use must result in a manipulative difference as compared to

the prior art. See *In re Casey*, 152 USPQ 235 (CCPA 1967) and *In re Otto*, 136 USPQ 458, 459

(CCPA 1963). Since such language does not limit a claim to a particular structure, it does not

limit the scope of a claim or claim limitation.

As per independent claims 2-17 Appellant relies on the arguments of claim 1 and they are

refuted as above.

As per claims 3, 7,10-14, the Appellant argues that the examiner fails to specify with

specificity the particular portions of the references meet such limitations. Appellant is directed

to column 24, lines 8-21 and other cited sections above under rejection of claims 3, 7 and 10-14.

The Appellant relies on its arguments for independent claim 1 to overcome the rejections

for dependent claims and claims 5-6 (specification page 10). Appellant's own specification

(page 1) in the background of invention, discloses that a "wide variety of cryptographic

techniques are known in the art...one well known type of public key cryptography is based on

ElGamal encryption. The Appellant further describes Schnorr signature as a well-known digital

signature scheme (specification page 1). In fact, Appellant's disclosure is evidence of such well-

known techniques to one of ordinary skill in the art to reject claims 5 and 6 without the need of

the additional reference (Zheng) cited by the examiner.

Therefore, in the view of the teachings, the examiner asserts that it would have been

obvious to one of ordinary skill in the art to modify Nishioka and utilize the teachings of

Kyojima with respect to blind decryption of signed ciphertext portion to further secure and

protect the privacy of a user from dissemination or interception of any data which does not

require disclosure to any entity but the user for completion of the electronic transaction.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

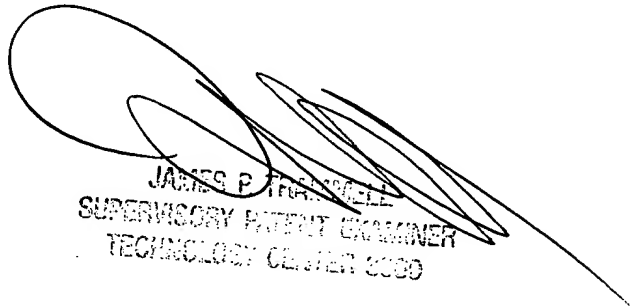Bradley Bayat
Examiner
Art Unit 3621

***
July 26, 2004

Conferees

James Trammell, SPE 3621

John Hayes, Primary Examiner 3621

Joseph B. Ryan
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560